METHOD AND SYSTEM OF TRANSACTION SECURITY

Priority Application

[0001] This application claims the benefit of U.S. Provisional Application No. 60/454,316 filed March 14, 2003, entitled "TRANSACTION SECURITY" and incorporated herein by this reference

Field of the Invention

[0002] The present invention relates generally to the field of transaction security, and more particularly to a method and system for secure authentication of a user in a transaction conducted electronically via sound, such as voice.

Background of the Invention

[0003] In order to provide security to transactions conducted via voice, e.g., over the telephone, it is often desirable to authenticate the speaker. One existing method for authenticating speakers in a telephone transaction is through a personal identification number (PIN) or telephone PIN (TPIN). While generally referred to as "PIN," the identification can be other than a number, e.g., a voiced phrase, an encoded data stream. Where this application refers to "voiced PIN," "keyed PIN," "PIN," "authentication information," etc., the full range of identification means are implied.

[0004] For example, a telephone banking user provides the PIN via voice or telephone keypad in order to inquire as to her account balance. Such an approach to authentication is subject to being compromised, for example, by a third party recording the voiced PIN or decoding the keyed PIN. The recorded or decoded information can then be used for unauthorized access to the account.

[0005] One potential solution involves voiceprint authentication, e.g., matching characteristics of a user's voice over the communications channel. Some embodiments of this approach use a training phrase, e.g., "open sesame." A user repeats the training phrase until sufficient characteristics of the user's voice saying the training phrase have been collected. When executing a transaction, the user speaks the training phrase (also referred to as a "pass phrase"); if the characteristics of the spoken training phrase matches the stored characteristics within an acceptable level of confidence, the user is authenticated. This approach is still open to exploitation by recording.

[0006] A variation on this approach relies on characteristics of the user's voice that are not specific to training phrases. This variation typically requires a much larger training set; the time required to obtain that training set may serve as a disincentive to enrollment. In addition, the processing resources required are likely much greater for this variation. Further, since the potential for false negatives and false positives is generally greater when the training is not based on a known set of pass phrases, this approach has a major disadvantage with respect to user acceptance.

[0007] Approaches have been developed to mitigate the risk of exploitation by record/playback of a speaker's authentication utterances. One such approach involves identifying telltale characteristics and limitations of a playback device (e.g. the absence or presence of special harmonics, modulations or other special signal characteristics) present in the play back of the illicitly recorded utterance (voice, PIN or otherwise). This approach would be effective only where the telltale characteristics were present within the bandwidth of the communication channel.

[0008] Another approach involves identifying the natural variation between separate instances of a spoken phrase. If such variations are not present, the risk that the utterance or TPIN is a recording is increased. Substantial variation would not be present between a high-fidelity recording and its spoken original, or between separate high fidelity playbacks of the same recording. Nevertheless, this approach can be defeated,

albeit requiring some technical sophistication, by introducing artificial variations – or in a lower-tech fashion by illicitly recording multiple versions of the spoken phrase.

[0009] Training on several different user phrases could be used to introduce diversity to the authentication phrase used in any specific transaction. Randomly alternating the required authentication response among the different phrases could be used. This diversity could mitigate the risk of false authentication but, as with other approaches, is susceptible to a reasonably persistent adversary who records multiple user authentication sessions. In addition, diversity among authentication phrases requires more training time, hence potentially less user acceptance.

Summary of the Invention

[0010] It is a feature and advantage of the present invention to provide a method and system for secure authentication of a user in a session conducted over an interactive communication channel, such as a two-way telephony communication channel, with an authenticating entity, such as a financial institution.

[0011] It is another feature and advantage of the present invention to provide a method and system for secure authentication of the user in a session conducted over an interactive communication channel that utilizes pseudorandom noise as a session identifier.

[0012] It is a further feature and advantage of the present invention to provide a method and system for secure authentication of the user in a session conducted over an interactive communication channel utilizing pseudorandom noise as a session identifier that enables the authenticating entity to determine whether or not authentication information for the user is a playback of a recording of an earlier session.

[0013] It is an additional feature and advantage of the present invention to provide a method and system for secure authentication of the user in a session conducted over an

interactive communication channel utilizing pseudorandom noise as a session identifier that enables an the authenticating entity, to determine whether or not authentication information for the user is a playback of a recording of an earlier session.

[0014] To achieve the stated and other features, advantages and objects, the present invention provides a method and system for secure authentication of a user in a session conducted over an interactive communication channel, such as a two-way telephony communication channel. An embodiment of the invention makes use of computer hardware and software and proposes that a user, such as a voice or touch tone keypad user, is allowed to access an authenticating entity, such as a financial institution, for example, via the two-way telephony communication channel.

[0015] Embodiments of the invention utilize for example, a two-way land line telephony communication channel, a two-way wireless telephony communication channel, or a two-way voice over Internet protocol (VoIP) telephony communication channel. Other embodiments of the invention utilize, for example, a two-way hard-wired telephony communication channel, a two-way satellite telephony communication channel, or a two-way microwave telephony communication channel.

[0016] When the user accesses the authenticating entity, the authenticating entity inserts a session identifier that is infeasible to detect or eliminate without knowledge of a secret known to the authenticating entity into the two-way telephony communication channel. In an embodiment of the invention, the session identifier is pseudorandom noise deterministically generated according to the secret known only to the authenticating entity, which secret consists, for example, of a pre-determined seed in combination with a pre-selected algorithm for generating the pseudorandom noise. In another embodiment, the session identifier is modulated by pseudorandom noise.

[0017] In an aspect of the invention, the session identifier can be inserted into the two-way telephony communication channel by the authenticating entity during an initial

personal identification number (PIN) training session for the user. In a further aspect of the invention, a different session identifier can be inserted into the two-way telephony communication channel by the authenticating entity during each subsequent session in which a PIN is entered for the user.

[0018] Authentication information for the user, such as the user's voice and/or PIN, can be entered by the user speaking and/or entering the authentication information on a touch tone keypad. Upon receiving the authentication information, the authentication information is analyzed by the authenticating entity to determine whether the session identifier inserted by the authenticating authority into the two-way telephony communication channel is associated with the received authentication information. If so, the authenticating entity can be certain that the authentication information is not a playback of a recording of an earlier session, and the user is authenticated by the authenticating entity based on the authentication information.

[0019] In the pseudorandom noise aspect of the invention in which the session identifier is pseudorandom noise, the authentication information is analyzed by the authenticating entity to determine whether the pseudorandom noise associated with the received authentication information is the same as the pseudorandom noise currently inserted by the authenticating authority into the two-way telephony communication channel. In this aspect, the pseudorandom noise associated with the authentication information is analyzed using the secret known to the authenticating entity that consists of the pre-determined seed in combination with the pre-selected algorithm used in generating the pseudorandom noise. If, for example, the analysis identifies pseudorandom noise inserted as a session identifier on a preceding occasion, the authenticating entity can be certain that the authentication information is a recording of the authentication information received on a preceding occasion.

[0020] Additional objects, advantages and novel features of the invention will be set forth in part in the description which follows, and in part will become more apparent

to those skilled in the art upon examination of the following, or may be learned from practice of the invention.

Brief Description of the Drawings

[0021] Fig. 1 is a schematic diagram that illustrates an example overview of key components and the flow of information between key components of the system for an embodiment of the present invention;

[0022] Fig. 2 is a flow chart that illustrates an example of the process of secure authentication of a user in a session conducted over a two-way telephony communication channel according to an embodiment of the present invention; and

[0023] Fig. 3 is a flow chart that illustrates an example of the process of secure authentication of a user in a session conducted over a two-way telephony communication channel according to another embodiment of the present invention.

Detailed Description

[0024] Referring now in detail to an embodiment of the present invention, an example of which is illustrated in the accompanying drawings, the present invention utilizes computer hardware and software to provide a method and system for secure authentication of a user in a session with an authenticating authority conducted electronically over an interactive communication channel, such as a two-way telephony communication channel, partly or entirely via voice.

[0025] In a preferred embodiment, a session identifier is inserted into the communication channel by the authenticating entity that cannot be easily detected or eliminated without knowledge of its construction (e.g. pseudorandom noise generated by a secret key known only to the authenticating entity). In some embodiments, the session

identifier is inserted during training and during each use of the voiced utterance or keyed PIN. Further embodiments inject pseudorandom noise into the communication channel.

[0026] Other embodiments inject a session identifier modulated by pseudorandom noise. Since the system of the authenticating entity knows the key to the pseudorandom stream, the system can recover the stream and data modulated thereon. In additional embodiments, the noise is not readily detectable to the voice user. Preferred embodiments are able to detect a subsequent illicit user playing back a recorded PIN by identifying a non-conforming identifier (e.g. a past, altered, unknown or missing session identifier).

[0027] Fig. 1 is a schematic diagram that illustrates examples of key components and the flow of information between the key components for an embodiment of the invention. Referring to Fig. 1, an embodiment of the invention involves a user 20, such as a voice user, at some type of communication device 22, such as a telephone, a wireless phone, or voice over IP, in which sounds or tones are modulated and converted to electronic analogues of electricity and modulated in whatever form is suitable for the transmission, for example, via satellite, microwave, landline, or the like. The user's communication device 22 is coupled , for example, via a two-way telephony channel of communication 24 to systems of an authenticating entity 26, such as a financial institution, on the receiving end, at which point, the modulated electronic signal is demodulated and converted back by a demodulating device 28, for example, to audio so the sound can be heard. In addition, at the receiving end, a session identifier generator 30, such as a pseudorandom noise generating device injects and also recovers or pulls out the injected signal from the communication channel 24.

[0028] Fig. 2 is a flow chart that illustrates an example of the process of secure authentication of a user in a session conducted over a two-way telephony communication channel according to an embodiment of the present invention. Referring to Fig. 2, at S1, the user 20 accesses the authenticating entity 26 via a two-way telephony communication

channel 24, and at S2, a system of the authenticating entity inserts a session identifier into the two-way telephony communication channel 24 that is infeasible to detect or eliminate without knowledge of a secret known only to the authenticating entity. At S3, authentication information for the user 20 is received by the authenticating entity's system via the two-way telephony communication channel 24, and at S4, the authentication information is analyzed by the authenticating entity's system to determine whether the session identifier inserted by the authenticating entity 26 into the two-way telephony communication channel 24 is associated with the received authentication information. At S5, if the session identifier is found to be associated with the authentication information, the user 20 is authenticated by the authenticating entity 26 based on the authentication information.

[0029] It is to be understood that the term "telephony" as used herein includes communication of information by means of electrical signals carried by wires or radio waves, in which voice or other sound is translated into electrical signals, transmitted, and then converted back into audio. The term "telephony" as used herein also refers to computer hardware and software that perform functions traditionally performed by telephone equipment.

[0030] The process of inserting an identifier, such as pseudorandom noise generated by a secret key known only to the authenticating entity 26, into the communication channel 24 is similar to generating a pseudorandom number. Although pseudorandom noise seems to lack a definite pattern, it consists of a sequence of signals that will usually repeat itself, for example, after a pre-determined period of time or a long series of signals.

[0031] In generating pseudorandom numbers, for example, a pre-selected seed is used with a particular algorithm to generate different numbers that appear to be random, but if an observer knows the seed and the algorithm for generating those apparently random numbers, the observer can actually algorithmically reproduce what the next

number in the sequence will be. From simply looking at the pseudorandom numbers, however, it is virtually impossible to reconstruct what the next number of the sequence will be without knowledge of the seed and the algorithm. To attempt to guess the seed by trial-and-error would be infeasible.

[0032] The term 'pseudorandom' is well-known, for example, in use of spread-spectrum systems. For example, in spread-spectrum systems, modulated carrier transmissions appear as random noise to a receiver that is incapable of correlating a locally generated pseudorandom code with the received signal. However, if one knows what the particular sequence is, for example, in sending a pre-determined number of bits (i.e., ones and zeros), then it is possible to add the signals up. Even though the signals have a very small magnitude, one is able to add them up and know the sequence in which they are being sent.

[0033] As used herein, the term 'pseudorandom noise' refers to an electronic signal that appears random but is instead a deterministically generated signal that is injected into the communication channel 24 and is difficult to distinguish from the underlying signal noise. It appears to be audible noise, for example, over a telephone line because the telephone converts the electronic signal into audible sound.

[0034] By adding up the signals , for example, every second, one who knows the sequence of how to add it up according to a particular predetermined phase shift or the like can uncover the signals being sought in the particular sequence. When the particular sequence is added up, the sum of the particular bits is larger than the surrounding noise and is thus distinguishable from it. On the other hand if one does not know the sequence which is being received, one would be unable to add up the signals, which would simply appear to be random noise.

[0035] In an embodiment of the invention, the pseudorandom noise is inserted in the communication channel 24, examples which include hard wired communication,

satellite communication, and microwave communication. Pseudorandom bits are modulated for transmission and sent via whatever communication channel is employed. Typically, a system receiving communication signals attempts to filter out the noise to eliminate background noise. Electronic noise sounds like audio noise, so attempts are made by the receiving system to filter it out. A system on the receiving end of the communications channel 24 will attempt to filter out that noise, which the system would interpret as noise.

[0036] Fig. 3 is a flow chart that illustrates an example of the process of secure authentication of a user in a session conducted over a two-way telephony communication channel according to another embodiment of the present invention. Referring to Fig. 3, at S10, when the user 20 accesses the authenticating entity 26 via a two-way telephony communication channel 24, for example, on a subsequent occasion, at S11, the authenticating entity again inserts a session identifier into the two-way telephony communication channel 24, but one that is different from the session identifier inserted during any previous session. At S12, authentication information for the user 20 is likewise received by the authenticating entity 26 via the two-way telephony communication channel 24, and at S13, the authentication information is likewise analyzed by the authenticating entity 26 to determine whether the session identifier currently inserted by the authenticating entity into the two-way telephony communication channel 24 is associated with the received authentication information. At S14, if the particular session identifier is found to be associated with the authentication information, the user 20 is again authenticated by the authenticating entity 26 based on the authentication information. However, at S15, if not, the user is not authenticated, and the authentication information can be analyzed further to determine which, if any, session identifier inserted by the authenticating entity 26 on a previous occasion is associated with the received authentication information. Thus, the authenticating entity 26 can determine which, if any, previous session was recorded and played back.

[0037] In an embodiment of the invention, a particular timed sample of a pre-defined sequence of pseudorandom noise is added up linearly to provide a much stronger signal, and if it matches the known pre-determined signal with phase shifts, and the like, it is known that the signal is a recorded replay. If a succeeding sequence adds up, for example, with phase shifts in a particular manner in the way in which it is expected, it is recognized as a particular sample of random noise injected into the communications channel 24.

[0038] Assume, for example, that there are 1000 bits in a sequence of pseudorandom noise and that the amplitude of the pseudorandom noise is 1000ths of the amplitude of the signal transmitted via the communication channel 24. Therefore, the amplitude of each instance of these bits is 1000ths of the amplitude of the signal and appears to be random noise in the receiving system. However, if one knows how to add up the bits and knows the sequence of the bits in the pseudorandom noise and how they were generated, for example, by frequency or amplitude modulation or the like, one can add up the bits in the correct manner. Then, the signal is 1000 times greater in magnitude than each individual bit because they have been added 1000 times. Thus, a strong signal of pseudorandom noise is seen in the system, because the bits have been added up in the particular sequence in which they are expected to appear in a particular secret pattern. This is the way in which signals are sent, for example, in spread-spectrum systems that enables multiple communications over the same physical channel without interfering with one another.

[0039] In an aspect of the invention, for example, a special training signal is sent with pseudorandom noise inserted which is below the level of the actual random noise in the communication channel 24. In another aspect, each time there is a communication via the communication channel 24, a different pseudorandom signal is inserted. Thus, each time a pseudorandom noise is sent with a communication via the communication channel 24, a different pseudorandom noise signal is inserted in the communication. If indeed what comes back to the authenticating entity 26 in the authentication information is the

same pseudorandom noise signal that was inserted in a previous communication, it would be known that the communication is a recording.

[0040] When the communication channel 24 is opened to the user 20, the pseudorandom noise signal is inserted that passes through any receiving system undetected because it appears to be below the typical signal to noise ratio. When the communication signal comes back to the authenticating entity 26, such as a financial institution, the pseudorandom noise signal is pulled from the communication signal because the predetermined sequence of the pseudorandom noise is known to the authenticating entity 26. The authenticating entity 26 can store, for example, the last *n* authentication communications, so if any one of the last *n* authentication communications were recorded and played back, it would be known to the authenticating entity 26 from the sequence that the current communication is a playback of one of the *n* previous communications.

[0041] While it is possible for a recording of a user's enrollment process to be made illicitly, such an occurrence is probably unlikely. However, it is more likely that such a recording could be made after enrollment when the user 20 routinely authenticates or verifies himself or herself by his or her voice print by speaking a phrase on which the authenticating entity's system is trained. Thus, an unauthorized person can tap into a landline communication channel 26 between the user 20 and the authenticating entity 26, such as the financial institution, or if the communication channel 24 is wireless, simply intercept the signal with a receiver, and record the user 20 speaking his or her authentication or verification phrase. The unauthorized person can simply dial in to the authenticating entity 26 at a later time and pretend he or she is the user 20, and when asked to speak the authentication or verification phrase, the unauthorized person can simply play the recording.

[0042] In an embodiment of the invention, present techniques of detecting such a recording include, for example, essentially looking for some unique characteristics of the

recording device, which is increasingly difficult because current technology enables recording devices with ever higher levels of fidelity to the original sound. An embodiment of the present invention is not dependent on matching the original sound pattern. Instead, each time the authenticating entity 26 sends its request to the user 20 to speak his or her authentication or verification, the communication is sent with pseudorandom noise sequences, modulations, phase shifts, or the like. For each time slot in which the modulations are done, the amplitude is very small, so it does not disturb the user 20 to hear it, and the sensitivity of the receiving system or a recording device will not filter it out. When the user 20 speaks the authentication or verification and it is sent back to the authenticating entity 26, the sequences are added up lineally in the correct phase, so that the pseudorandom noise signal is recovered in addition to the user's verification phrase.

[0043] In other words, the verification phrase plus the pseudorandom noise signal is received by the authenticating entity 26 from the user 20. The authenticating entity 26 knows what the pseudorandom noise signal was when the user 20 was verified on preceding occasions. The next time the user 20 calls in to be authenticated or verified, the authenticating entity 26 inserts a different pseudorandom noise sequence into the system. So, if the authenticating entity 26 pulls out of the user's current verification phrase and determines that it is not associated with the pseudorandom noise sequence that was currently sent to the user 20, but is instead associated with a pseudorandom noise sequence for a preceding session, it is readily apparent to the authenticating entity 26 that the current verification is a recorded playback.

[0044] The number of preceding verifications that are stored by the authenticating entity 26 for comparison varies, depending how far back the authenticating entity 26 wants to compare. If, for example, ten preceding verifications are retained in storage, each with its own unique pseudorandom noise sequence inserted, the current verification can then be compared not only with the current pseudorandom noise sequence, but also with any or all of the ten preceding verifications. Each pseudorandom noise signal is

added up lineally in the correct fashion to see if the result is a pseudorandom noise signal from one of those preceding ten verifications, and if so, the authenticating entity 26 knows that the current verification is a recording, and moreover, the authenticating entity 26 knows precisely which preceding verification was recorded.

[0045] Various preferred embodiments of the invention have been described in fulfillment of the various objects of the invention. It should be recognized that these embodiments are merely illustrative of the principles of the present invention. Numerous modifications and adaptations thereof will be readily apparent to those skilled in the art without departing from the spirit and scope of the present invention.

[0046] What is claimed is: